

In the Claims

The status of claims in the case is as follows:

1 1. [Currently amended] A system for a web based trust
2 model governing delivery of services and programs from a
3 workflow, enterprise and mail-enabled application server and
4 platform, comprising:

5 a connection protocol connecting a user client to a
6 server site;

7 download utilities responsive to said connection
8 protocol for downloading said services and programs
9 from said server site to separate and non-conflicting
10 execution spaces at said user client; [[and]]

11 trust assignment user interface dialogs responsive to
12 said connection protocol for advising said user of
13 risks taken when accepting executable download from
14 said server site; and

15 said server site responsive to said user accepting said

16 server site as trusted for centrally administering
17 security policies for said services and programs
18 executing at said user client.

1 2. [Original] The system of claim 1, said connection
2 protocol selectively being HTTP or HTTPS.

1 3. [Original] The system of claim 1, further comprising:

2 a processor for establishing security context, said
3 processor including

4 a stage 1 processor for determining from said user
5 if said server site is to be trusted; and

6 a stage 2 processor for establishing whether or
7 not the identity of said web site is confirmed and
8 determining from said user if processing should
9 continue to include installation of programs on
10 said client.

1 4. [Original] The system of claim 3, further comprising:

2 a client download page;

3 a download control element in said download page;
4 said processor being activated upon activation of said
5 download control element within said download page
6 initiating a download process first to establish a
7 security context and then to download program
8 executable files.

1 5. [Original] The system of claim 2, further comprising:
2 said download utilities being responsive to an SSL
3 connection to said server for activating said dialog to
4 advise said user that said server site has been
5 verified as being what it represents itself to be and
6 to query said user whether code is to be downloaded
7 from said server site to said client.

1 6. [Original] The system of claim 5, said code being
2 custom code.

1 7. [Previously amended] The system of claim 5, said
2 download utilities being responsive to a connection from
3 said client to said server being other than SSL for
4 activating said dialog to advise said user that said server

5 site has not been verified as being what it represents
6 itself to be and to query said user whether code is to be
7 downloaded from said server site to said client.

1 8. [Original] The system of claim 7, said code being
2 custom code.

1 9. [Original] The system of claim 1, further comprising:

2 said download utilities being responsive to user
3 acceptance of download from said server site of
4 executable code for downloading said executable code to
5 said client;

6 a trace utility for identifying originators of
7 downloaded code.

1 10. [Original] The system of claim 9, said trace utility
2 selectively identifying originators of signed agents through
3 electronic signature, of custom code traceable to code
4 vendor through web site relationship, or custom code
5 directly created by said web site.

1 11. [Original] The system of claim 1, further comprising:

2 a first trust model for establishing level of traceable
3 accountability for a subscription at download time over
4 a secure connection protocol;

5 a second trust model for establishing a reduced level
6 of traceable accountability, with traceable
7 accountability established only for electronically
8 signed agents used by said subscription over a
9 connection protocol not verified as secure; and

10 said dialogs being responsive to said trust models.

1 12. [Previously amended] A method for governing delivery
2 of services and programs from a workflow, enterprise and
3 mail-enabled application server and platform according to a
4 web based trust model, comprising the steps of:

5 establishing a connection protocol between a client and
6 a web site;

7 responsive to said connection protocol, determining a
8 trust level assignable to said web site relative to
9 risks taken when accepting executable download from
10 said web site;

11
12 advising a user at said client of said trust level
13 assignable with respect to said risks to said web site;
14 and
15
16 responsive to user acceptance of said risks and
17 accepting said server site as trusted, downloading said
18 services and programs from a server site to separate
19 and non-conflicting execution spaces at said user
20 client and centrally administering security policies
21 for said services and programs executing at said
22 client.

1 13. [Original] The method of claim 12, further comprising
2 the steps of:

3 displaying a download control element in a client
4 download page;

5 responsive to user selection of said download control
6 element or upon schedule, initiating a download process
7 first to establish a security context and then to
8 download program executable files from said server.

1 14. [Original] The method of claim 12, further comprising
2 the step of:

3 responsive to user acceptance of download from said
4 server site of executable code, downloading said
5 executable code to said client.

1 15. [Original] The method of claim 14, further comprising
2 the step of:

3 identifying originators of downloaded code.

1 16. [Original] The method of claim 15, further comprising
2 the step of

3 selectively identifying originators of signed agents
4 through electronic signature, of custom code traceable
5 to code vendor through web site relationship, or custom
6 code directly created by said web site.

1 17. [Previously amended] The method of claim 12, further
2 comprising the steps of

3 establishing a first trust model specifying a level of

traceable accountability for a subscription at download
time over a secure connection protocol;

establishing a second trust model for specifying a
reduced level of traceable accountability, with
traceable accountability established only for
electronically signed agents used by said subscription
over a connection protocol not verified as secure; and

said dialogs being responsive to said trust models.

18. [Previously amended] A program storage device readable
by a machine, tangibly embodying a program of instructions
executable by a machine to perform method steps for
governing delivery of services and programs from a workflow,
enterprise and mail-enabled application server and platform
according to a web based trust model, said method steps
comprising:

establishing a connection protocol between a client and
a web site;

responsive to said connection protocol, determining a
trust level assignable to said web site relative to

12 risks taken when accepting executable download from
13 said web site;

14 advising a user at said client of said trust level
15 assignable with respect to said risks to said web site;
16 and

17 responsive to user acceptance of said risks and
18 accepting said server site as trusted, downloading said
19 services and programs from a server site to separate
20 and non-conflicting execution spaces at said user
21 client and centrally administering security policies
22 for said services and programs for centrally
23 determining and controlling services and programs to be
24 executed at said client.

1 19. [Previously amended] A computer program product
2 configured to be operable to govern delivery of services and
3 programs from a workflow, enterprise and mail-enabled
4 application server and platform according to a web based
5 trust model, according to the steps of:

6 establishing a connection protocol between a client and
7 a web site;

8 responsive to said connection protocol, determining a
9 trust level assignable to said web site relative to
10 risks taken when accepting executable download from
11 said web site;

12 advising a user at said client of said trust level
13 assignable with respect to said risks to said web site;
14 and

15 responsive to user acceptance of said risks and
16 accepting said server site as trusted, downloading said
17 services and programs from said server site to separate
18 and non-conflicting execution spaces at said user
19 client and centrally administering from said server
20 site security policies for control which said services
21 and programs shall be executed at said client.